Reference Implementation: GSC-IS 2.1

Joe Broghamer

Department of Homeland Security
Office of the Chief Information Officer

dhscio.net
   (temporary secure Web site)

Introduction

- Standards
  - Industrial Standards
    - Formal (ex: USB, FireWire, 802.11, Bluetooth)
    - Market share (MS Outlook in Corporations)
    - Government standards (NIST, DIN)
- Reference Implementation
  - Prove compliance to standards
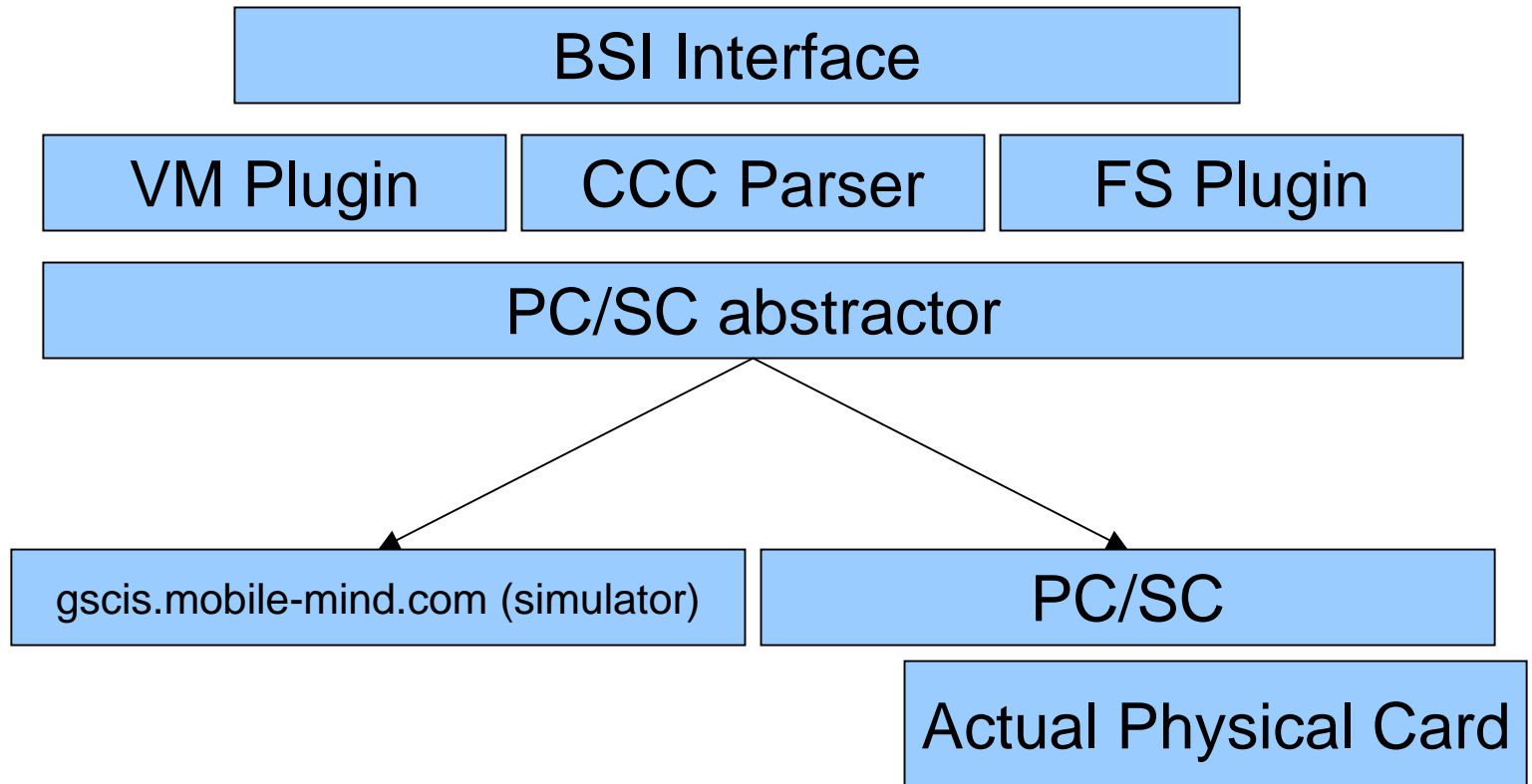 - Demonstrate interoperability

Goal

- NIST has undergone the development of a reference implementation of GSC-IS 2.1
  - To provide a reference BSI that can communicate with both native GSC-IS 2.1 VM and File System cards
  - To provide a reference GSC-IS 2.1 simulator for VM and File System like card edges.
  - To surface ambiguities in the current GSC-IS 2.1 specification and provide guidance for implementors

Architecture

BSI Interface

VM Plugin	CCC Parser	FS Plugin

PC/SC abstractor

gscis.mobile-mind.com (simulator)	PC/SC

	Actual Physical Card

Card-Edge simulators

- Progress
  - VM "usage" simulator completes GSC-IS 2.1 specification as it is today
    - Need to address personalization (card management)
    - Potential to test reference applets on actual cards instead of a simulator
  - File system "usage" simulator completes GSC-IS 2.1 specification as is
    - Some personalization already addressed using ISO standards
  - Simulators provide native GSC-IS 2.1 implementation so no APDU translation is needed

BSI

- Progress
  - Currently addresses VM "usage" in accordance with current GSC-IS 2.1 specification.
  - Usage is tested with sample data provided with the reference implementation simulator
  - File system card edge support in progress
  - BSI currently does no APDU translation and assumes a native GSC-IS 2.1 implementation.

Moving forward

- Need to determine how the reference implementation might support the Homeland Security Presidential Directive (HSPD)
- How to unify ANSI, ISO, HSPD, and GSC-IS 2.1
- Look at how the reference implementation can be used to provide guidance for backward compatibility for current deployments
- Look at how the reference implementation can be used for compliance testing of platforms (middleware, cards, applets, etc)
- Encourage direct support from OS vendors